

Regulation EU 2023/1113 and FATF R16: Travel Rule for Funds and Crypto-Assets

30 August – 10 September 2027
Kuala Lumpur (Malaysia)

UK Training

PARTNER



Regulation EU 2023/1113 and FATF R16: Travel Rule for Funds and Crypto-Assets

Ref: 3255553_344679 **Date:** 30 August – 10 September 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 8800 GBP

Regulation EU 2023/1113 and FATF R16, FATF Recommendation 16, set out the Travel Rule for funds and crypto-assets: the payer, payee, originator and beneficiary data that must accompany each transfer between providers. This 10-day course is for compliance, anti-money laundering and payments operations professionals at banks, payment institutions and crypto-asset service providers, and its final deliverable is a Travel Rule control file.

Introduction

The course rests on three texts. Regulation EU 2023/1113 is the law on information accompanying transfers of funds and certain crypto-assets; it repeals the earlier transfer of funds rules and extends them to crypto-asset service providers CASPs. The EBA Travel Rule Guidelines EBA/GL/2024/11 explain how providers detect and handle missing information. FATF Recommendation 16, now titled Payment transparency, is the international standard behind both. The level is intermediate: delegates already know basic anti-money laundering duties. Teaching uses case studies and transfer simulations from banking, e-money and crypto-asset exchanges.

Course Objectives

- Define the data that must accompany a transfer of funds and a crypto-asset transfer under Regulation EU 2023/1113
- Distinguish a payment service provider from a CASP, and an intermediary from an end provider, when assigning Travel Rule duties
- Compare hosted and self-hosted addresses and apply the ownership or control assessment where the Regulation requires it
- Interpret the EBA Travel Rule Guidelines to decide whether a deficient transfer is executed, rejected or suspended
- Compare the original and revised FATF Recommendation 16 and map the differences to an existing control set
- Justify Travel Rule controls and records to internal audit and supervisors with evidence

The graphic features the text 'UK Training' in a small, grey font above the word 'PARTNER' in a large, bold, black font. This text is positioned over a background of concentric grey circles and a chessboard pattern. In the foreground, three chess pieces—a silver pawn, a silver knight, and a gold king—are visible on the chessboard squares.

UK Training
PARTNER

Target Audience

- Bank and payment institution compliance officers who must decide how far existing controls cover the extended Travel Rule
- Anti-money laundering officers at crypto-asset service providers who must judge when a self-hosted address needs an ownership check
- Payments and crypto operations leads who must choose how to treat a transfer with missing data
- Risk and internal control professionals who must select the indicators that show Travel Rule data quality
- Internal auditors and legal advisers who must interpret whether procedures meet the Regulation and the guidelines
- Product and technology owners who must select messaging tools that carry party data

Course Outline

Day 1: Travel Rule Foundations and the Move to Regulation EU 2023/1113

- Travel Rule vs Customer Due Diligence: Data That Moves With Each Transfer
- Regulation EU 2023/1113: Scope Covering Transfers of Funds and Certain Crypto-Assets
- Repealed Regulation EU 2015/847: Earlier Rules Limited to Funds Without Crypto-Assets
- FATF Recommendation 16 vs Recommendation 15: Payment Transparency and Virtual Asset Standards
- Money Laundering and Fraud Typologies: How Opaque Transfers Conceal Illicit Flows

Day 2: Who Is in Scope: Payment and Crypto-Asset Service Providers

- PSP vs Intermediary PSP: Roles Along a Chain of Fund Transfers
- CASP vs Intermediary CASP: Roles When Crypto-Assets Pass Through Several Providers
- In-Scope Transfer Test: Deciding Whether a Transaction Triggers Travel Rule Obligations
- Card Purchase Exemption: Where Revised Recommendation 16 Obligations Stop Applying
- Cross-Sector Scope Exercise: Classifying Bank, E-Money and Exchange Transactions

Day 3: Information Accompanying Transfers of Funds

- Payer vs Payee Information: Data Items Required for Each Party
- Domestic vs Cross-Border Fund Transfers: Comparing the Data Each Route Must Carry
- Payment Message Fields: Mapping Payer and Payee Data Into Structured Formats
- Data Accuracy and Verification: Checking Payer Identity Before Funds Are Sent
- Batch File Transfers: Carrying Complete Party Data for Grouped Payments

UK Training

PARTNER



Day 4: Originator and Beneficiary Data for Crypto-Asset Transfers

- Originator vs Beneficiary Information: Data Items for Each Crypto-Asset Transfer
- No Minimum Amount Rule: Why Every Crypto-Asset Transfer Carries Party Data
- Distributed Ledger Address and Account Number: Identifying Parties in Crypto-Asset Transfers
- Data Transmission Timing: Sending Party Information Before or With the Transfer
- Messaging Protocols vs Bilateral Exchange: Options for Passing Data Between CASPs

Day 5: Self-Hosted Addresses and Counterparty Checks

- Hosted vs Self-Hosted Address: Telling Provider Wallets From Customer-Controlled Wallets
- Article 145 vs Article 162: Originator-Side and Beneficiary-Side Self-Hosted Duties
- Ownership or Control Assessment: Transfers Above the Threshold to Self-Hosted Addresses
- Acceptable Verification Methods: Guidance on Proving Control of a Self-Hosted Address
- Counterparty CASP Due Diligence: Assessing a Receiving Provider Before Sending Data

Day 6: Missing, Incomplete and Inconsistent Information

- Missing vs Incomplete Information: Distinguishing Absent Data From Meaningless Entries
- Execute, Reject or Suspend: Risk-Based Responses to Deficient Incoming Transfers
- Persistently Failing Providers: Warnings, Restrictions and Reporting of Counterparties
- Suspicious Transaction Reporting: Linking Information Gaps to Financial Intelligence Escalation
- Ex-Post Monitoring vs Real-Time Screening: Detecting Gaps Before and After Execution

Day 7: Applying the EBA Travel Rule Guidelines

- EBA/GL/2024/11 vs JC/GL/2017/16: What the Travel Rule Guidelines Replaced
- Policies and Procedures Under the Guidelines: Documenting Each Travel Rule Decision
- Intermediary Provider Duties: Passing On Information Without Alteration or Loss
- Interoperability Between Messaging Solutions: Handling Counterparties on Different Protocols
- Record-Keeping and Audit Trail: Retaining Transfer Data for Supervisory Review

Day 8: Revised FATF Recommendation 16 and Payment Transparency

- Original vs Revised Recommendation 16: From Terrorist Financing Focus to Payment Transparency
- Fraud and Error Protection Tools: Safeguards the Revised Standard Introduces
- Methodology Annex IV: How Mutual Evaluations Assess Revised Recommendation 16
- Gap Mapping Exercise: Comparing Regulation EU 2023/1113 Duties With Revised FATF Text
- Implementation Horizon Planning: Sequencing Changes Ahead of National Adoption

UK Training

PARTNER



Day 9: Controls, Governance and Supervisory Readiness

- First Line vs Second Line Controls: Ownership of Travel Rule Checks
- Key Risk Indicators: Measuring Data Completeness and Counterparty Failure Rates
- Staff Training and Escalation Roles: Assigning Travel Rule Responsibilities Across Teams
- Supervisory Inspection Preparation: Common Findings and the Evidence Requested
- Technology Selection: Screening Tools, Messaging Providers and Blockchain Analytics

Day 10: Travel Rule Case Simulation and Control File

- Bank vs Crypto Exchange Case: Applying Scope Tests to Mixed Transfer Flows
- Deficient Transfer Simulation: Applying the Execute, Reject or Suspend Decision Tree
- Self-Hosted Address Case: Applying Ownership Checks to a Withdrawal Request
- Peer Review of Controls: Testing Procedures Against Revised Recommendation 16 Gaps
- Travel Rule Control File: Finalising the Procedure, Decision Matrix and Data Map

Skills You Will Gain

- Travel Rule Scope Assessment
- Originator and Beneficiary Data Mapping
- Self-Hosted Address Verification
- Counterparty CASP Due Diligence
- Missing Information Handling
- Payment Transparency Gap Analysis
- Travel Rule Record-Keeping
- Supervisory Evidence Preparation

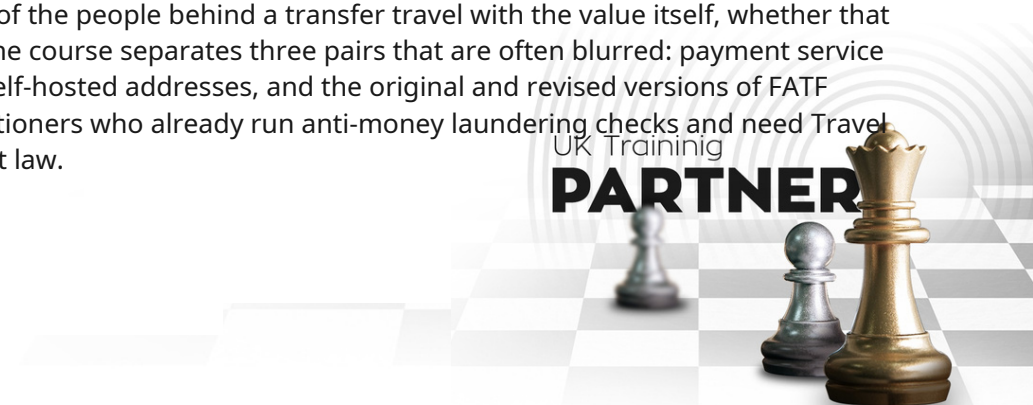
Why Attend This Course

- From controls built only for bank payments to one approach covering transfers of funds and crypto-asset transfers alike
- From treating every wallet the same to separating hosted and self-hosted addresses and checking ownership where required
- From case-by-case reactions to incomplete data to a documented execute, reject or suspend decision route
- From scattered notes on the old rules to a finished Travel Rule control file with a procedure, decision matrix and data map

Conclusion

The Travel Rule makes the identity of the people behind a transfer travel with the value itself, whether that value is money or a crypto-asset. The course separates three pairs that are often blurred: payment service providers and CASPs, hosted and self-hosted addresses, and the original and revised versions of FATF Recommendation 16. It suits practitioners who already run anti-money laundering checks and need Travel Rule procedures that reflect current law.

UK Training
PARTNER

A graphic of a chessboard with several chess pieces (a king, a queen, a rook, and a pawn) positioned on the board, set against a background of concentric circles.

Course FAQs

What is the Travel Rule under Regulation EU 2023/1113?

It is the duty on payment and crypto-asset service providers to send, check and keep defined data about the parties to each transfer of funds or crypto-assets, so that every transfer can be traced back to a payer or originator and forward to a payee or beneficiary.

What is the difference between a hosted and a self-hosted address in the crypto-asset Travel Rule?

A hosted address is held for a customer by a CASP, so the counterparty provider exchanges party data. A self-hosted address is controlled by the user, so no provider receives the data, and above the Regulation's threshold the CASP must assess who owns or controls it.

Which standards does the Regulation EU 2023/1113 and Travel Rule course follow?

It follows Regulation EU 2023/1113, the EBA Travel Rule Guidelines EBA/GL/2024/11 and FATF Recommendation 16 on payment transparency, read alongside Recommendation 15 for virtual assets, comparing the regional legal duties with the international standard at each step.

Is the Regulation EU 2023/1113 and Travel Rule course right for an AML officer at a crypto-asset service provider?

Yes. Anti-money laundering officers at CASPs work through originator and beneficiary data, self-hosted address checks, counterparty due diligence and missing-information decisions, alongside bank and payment cases.

What do delegates produce in the Travel Rule for fund and crypto-asset transfers course?

Each delegate completes a Travel Rule control file: a written procedure, a decision matrix for missing or incomplete information, and a data map showing which party data each transfer type carries between providers.

UK Training

PARTNER

A graphic of a chessboard with several chess pieces (king, queen, rook, knight, and pawns) in gold and silver, set against a background of concentric circles.